IN THE CLAIMS:

Please amend Claims 1, 8, 18, 25, 35, and 37 as follows.

1. (Currently Amended) An information processing apparatus comprising:

first input means for inputting encoded data of information data consisting of plural frames;

second input means for inputting security data for protecting at least one section of the information data;

extraction means for extracting a start code of a frame group consisting of at least one frame, from the encoded data included in the section for which security is set and which is to be protected in accordance with the security data, wherein the start code is a code discriminable from the encoded data;

superimposing means for superimposing the security data related to the frame group to which the start code belongs, on ~~the~~ said start code;

and

output means for outputting the encoded data processed by scrambling means for scrambling the encoded data other than the start code in the section for which the security is set.

2. (Previously Presented) An apparatus according to Claim 1, wherein the security data contains key information to be used by the scrambling means.

3. (Original) An apparatus according to Claim 1, wherein the security data contains information for an authentication process.

4. (Previously Presented) An apparatus according to Claim 1, wherein the information data is image data, and the encoded data includes an MPEG-4 bitstream.

5. (Original) An apparatus according to Claim 4, further comprising IPMP encoding means for generating IPMP data indicating information that pertains to the security, and wherein said output means outputs the IPMP data generated by said IPMP encoding means.

6. (Original) An apparatus according to Claim 1, further comprising enciphering means for enciphering the security data, and wherein said superimposing means superimposes the security data enciphered by said enciphering means.

7. (Previously Presented) An apparatus according to Claim 1, wherein the start code of the frame group comprising at least one frame is a start code of a predetermined frame, a start code of a predetermined frame group, or a start code of a predetermined sequence.

8. (Currently Amended) An information processing apparatus comprising:

input means for inputting image encoded data comprising:

a start code of a frame group, comprising at least one frame, the start code of the frame group including security data adaptively superimposed thereon; and

image encoded data other than the start code that is adaptively scrambled in accordance with the security data,

wherein the security data comprises data for protecting at least a part of the image encoded data;

code extraction means for extracting from the image encoded data a code which is located at a position where the start code is present, wherein the start code is a code discriminable from the encoded data;

detection means for detecting the security data from the extracted code;

descrambling means for descrambling the image encoded data other than the start code that is adaptively scrambled, in accordance with a detection result of said detection means; and

decoding means for decoding the image encoded data descrambled by said descrambling means.

9. (Previously Presented) An apparatus according to Claim 8, wherein the security data contains authentication data to be used to check the authenticity of the security data, and said apparatus further comprises authentication means for checking the authenticity of the security data.

10. (Previously Presented) An apparatus according to Claim 9, wherein said descrambling means descrambles the scrambled image encoded data in accordance with a checking result of said authentication means.

11. (Previously Presented) An apparatus according to Claim 8, wherein the security data is enciphered security data, and said apparatus further comprises deciphering means for deciphering the enciphered security data.

12. (Previously Presented) An apparatus according to Claim 8, wherein the image encoded data is MPEG-4 bitstream data.

13. (Original) An apparatus according to Claim 12, wherein said input means inputs IPMP data indicating information which pertains to security.

14. (Previously Presented) An apparatus according to Claim 13, wherein the IPMP data contains authentication data to be used to check the authenticity of the security data, and said apparatus further comprises authentication means for checking the authenticity of the security data in accordance with the authentication data.

15. (Previously Presented) An apparatus according to Claim 14, wherein said descrambling means descrambles scrambled image encoded data in accordance with a checking result of said authentication means.

16. (Previously Presented) An apparatus according to Claim 15, wherein the security data is enciphered data, and said apparatus further comprises deciphering means for deciphering the enciphered security data.

17. (Previously Presented) An apparatus according to Claim 8, wherein the start code of the frame group comprising the at least one frame is a start code of a predetermined frame, a start code of a predetermined frame group, or a start code of a predetermined sequence.

18. (Currently Amended) An information processing method comprising the steps of:

inputting encoded data of information data consisting of plural frames;

inputting security data for protecting at least one section of the information data;

extracting a start code of a frame group consisting of at least one frame from the encoded data included in the section for which security is to be set and which is to be protected in accordance with the security data, wherein the start code is a code discriminable from the encoded data;

superimposing the security data related to the frame group to which the start code belongs, on ~~the~~ said start code;

and

outputting the encoded data processed in a step of scrambling the encoded data other than the start code in the section for which the security is set.

19. (Previously Presented) A method according to Claim 18, wherein the security data contains key information to be used in the scrambling step.

20. (Original) A method according to Claim 18, wherein the security data contains information for an authentication process.

21. (Previously Presented) A method according to Claim 18, wherein the encoded data includes an MPEG-4 bitstream.

22. (Original) A method according to Claim 21, further comprising an IPMP encoding step of generating IPMP data indicating information that pertains to the security, and wherein said output step includes a step of outputting the IPMP data generated in the IPMP encoding step.

23. (Previously Presented) A method according to Claim 18, further comprising an enciphering step of enciphering the security data, and wherein said superimposing step includes a step of superimposing the security data enciphered in said enciphering step on the start code.

24. (Previously Presented) A method according to Claim 18, wherein the start code of the frame group comprising the at least one frame is a start code of a predetermined frame, a start code of a predetermined frame group, or a start code of a predetermined sequence.

25. (Currently Amended) An information processing method comprising the steps of:

inputting image encoded data comprising:

a start code of a frame group comprising at least one frame, the start code of the frame group including security data adaptively superimposed thereon; and

image encoded data other than the start code that is adaptively scrambled in accordance with the security data,

wherein the security data comprises data for protecting at least a part of the image encoded data;

extracting from the image encoded data a code which is located at a position where the start code is present, wherein the start code is a code discriminable from the encoded data;

detecting the security data from the extracted code;

descrambling the image encoded data other than the start code in accordance with the detection result of said detecting step; and

decoding the descrambled image encoded data.

26. (Previously Presented) A method according to Claim 25, wherein the security data contains authentication data to be used to check the authenticity of the security data, and said method further comprises an authentication step of checking the authenticity of the security data.

27. (Previously Presented) A method according to claim 26, wherein said descrambling step includes a step of descrambling scrambled image encoded data in accordance with a checking result in said authentication step.

28. (Original) A method according to Claim 25, wherein the security data is enciphering data, and said method further comprises as deciphering step of deciphering the enciphered security data.

29. (Previously Presented) A method according to Claim 25, wherein the image encoded data is MPEG-4 bitstream data.

30. (Previously Presented) A method according to Claim 29, wherein said inputting step includes a step of inputting IPMP data indicating information which pertains to security.

31. (Previously Presented) A method according Claim 30, wherein the IPMP data contains authentication data to be used to check the authenticity of the IPMP data, and

said method further comprises an authentication step of checking the authenticity of the IPMP data in accordance with the authentication data.

32. (Previously Presented) A method according to Claim 31, wherein said descrambling step includes a step of descrambling scrambled image encoded data in accordance with a checking result in said authentication step.

33. (Original) A method according to Claim 31, wherein the security data is enciphered data, and said method further comprises a deciphering step of deciphering the enciphered security data.

34. (Previously Presented) A method according to Claim 25, wherein the start code of the frame group comprising the at least one frame is a start code of a predetermined frame, a start code of a predetermined frame group, or a start code of a predetermined sequence.

35. (Currently Amended) An information processing method comprising the steps of:

inputting image encoded data that forms a hierarchical structure;

extracting a start code indicating a head of a predetermined layer from the image encoded data, wherein the start code is a code discriminable from the image encoded data; and

superimposing security data for protecting at least a part of an image onto the start code extracted in said extracting step.

36. (Original) A method according to Claim 35, further comprising an enciphering step of enciphering the image encoded data in accordance with the security data.

37. (Currently Amended) An information processing method comprising the steps of:

inputting encoded data in which security data for protecting at least a part of an image is superimposed on a start code indicating a head of a predetermined layer of image encoded data that forms a hierarchical structure, wherein the start code is a code discriminable from the encoded data;

extracting from the encoded data a code which is located at a position where the start code is present;

detecting the security data from the extracted code; and

decoding the encoded data in accordance with a detection result in said detecting step.

38. (Original) A method according to Claim 37, wherein the encoded data is enciphered data, and said decoding step includes a step of deciphering the enciphered encoded data.

39. (Previously Presented) A computer readable storage medium which stores a control program that implements an information processing method recited in Claim 18.

40. (Previously Presented) A computer readable storage medium which stores a control program that implements an information processing method recited in Claim 25.

41. (Previously Presented) A computer readable storage medium which stores a control program that implements an information processing method recited in Claim 35.

42. (Previously Presented) A computer readable storage medium which stores a control program that implements an information processing method recited in Claim 37.